STRATEGY RESEARCH PROJECT

INFORMATION OPERATIONS

BY

LIEUTENANT COLONEL PETER L. BURNETT JR.
United States Army

USAWC CLASS OF 2002

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

INFORMATION OPERATIONS

by

Peter L. Burnett Jr.
U.S. Army

COL James E. Gordon
Project Advisor

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: LTC Peter L. Burnett Jr.

TITLE: Information Operations

FORMAT: Strategy Research Project

DATE: 09 April 2002 PAGES: 36 CLASSIFICATION: Unclassified

This SRP proposes designation of a single entity within the federal government to provide strategic guidance across the breadth of the nation's elements of power. It would coordinate and improve the security of the nation's critical information infrastructure, which is essential for the survival and prosperity of the United States.

A review of the recent terrorist activities in the United States and the declaration of war against global terrorism revealed U.S. weakness in its ability to protect itself internally against terrorist activities. The United States found itself lacking in numerous areas. Area shortfalls include a lack of structure and policy and, in some cases, organizational structure that is focused on Homeland Defense. The U.S. also revealed an inability to protect its citizens, its physical infrastructures, the nation's economic structure, and critical information infrastructures. Numerous policies regarding domestic terrorist have been written and debated, but shelved. Older policy focused mostly on deterring terrorism and defeating terrorism abroad. On 11 September 2001, America witnessed terror firsthand in a well orchestrated attack that ripped and tore the economic and military fabric of its foundation. This event has prompted U.S. leaders to take a serious look internally at securing the liberty and prosperity of the nation's foundation. This study proposes ways and means of utilizing and protecting U.S. information operations in the war on terrorism.

TABLE OF CONTENTS

PREFACE

This paper will define Information Operations as it relates to securing the U.S. critical information infrastructure. It will review relevant Presidential Decision Directives, as well as regulatory and policy guidance and joint publications doctrine for guidance to IO; analyze challenges to the system; and discuss using the office of Homeland defense to strategically organize Information Operations (IO). It concludes with recommendations to enhance the security of the nation's critical information infrastructure.

Definition
"Information operations (IO) consist of actions taken to affect adversary's information and information systems while defending one's own information and information system."
The definition of Information Operations is so broad that the meaning of IO encompasses many variables to include targets, weapons, resources, or domain of operations. This definition also suggests activities such as collecting, processing, analyzing, and disseminating information while building an IO campaign to be integrated in support of offensive or defensive operations. The definition of Information Operations encompasses many activities. The principal function of IO is divided into offensive and defensive measures that support the national military strategy. Information Operations is the newest function being defined within the Department of Defense (DOD) as well as across the Federal Government. Theoretical discussion of the function of IO has caused a lot of anxiety within DOD and the Federal Government. A close review of IO background and current policy will provide doctrinal foundation for employment of IO in support of national military strategy and Homeland Defense.

LIST OF ILLUSTRATIONS

LIST OF TABLES

INFORMATION OPERATIONS

BACKGROUND AND CURRENT POLICY

The December 2000, National Security Strategy (NSS) is the nation's current strategy document. It sets our goals and objectives for protecting America's interests and identifies threats that impact the protection of those interests at home and abroad. The NSS mandates actions that will provide "a stable, peaceful international security environment as the desired end state — one in which our nation, citizens and interests are not threatened."[1]

To ensure this desired end state, one of our nation's objectives are to "...enhance security at home and abroad."[2] This statement hit home after the terrorist attack on the World Trade Center complex and the Pentagon using two American airplanes, as well as a failed attack using a third American airplane that crashed in the hills of Pennsylvania. Although mandates and plans were in place to secure the nation, the nation was not prepared for what it experienced on 11 September 2001. Therefore, measures were reviewed and taken by the President and Congress to secure and protect the interest of the nation. The policies that are currently in effect recommend the following:

Presidential Decision Directive – PDD 39: The U.S. Policy on Counterterrorism. This policy would "deter, defeat, and respond vigorously to all terrorist attacks on our territory and against our citizens, or facilities, whether they occur domestically, in international waters or airspace or on foreign territory."[3]

Presidential Decision Directive - PDD 62: This policy calls for protection against Unconventional Threats to Homeland and Americans Overseas. The President directs a coordinated effort with our friends and allies abroad. He seeks to strengthen law enforcement and put counter terrorism tools in place that would improve the security of airports and airplanes. The Office of the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism has the responsibility to keep the President informed of all changes in this area. [4]

Presidential Decision Directive – PDD 63: Critical Infrastructure Protection. This policy directs our agencies to "maintain the ability to protect the nation's critical infrastructures from intentional acts that significantly diminish the abilities of the Federal Government to perform national security missions." [5]

Clearly the President is focused on what needs to be done to secure the nation's critical information infrastructures. The question becomes whether Congress, governmental agencies,

private agencies and the nation's leadership remains focused on what needs to be done to ensure the security and survivability of the country as well as the infrastructures. The directives provide the framework, but the capability to succeed and maintain focus will determine our success. The key to protecting the nation's critical information infrastructure will depend heavily on the leadership and management of IO organizations to execute Presidential guidance provided in the directives and avoid getting lost in bureaucratic red tape and regulatory issues.

REGULATORY GUIDANCE

Defending America's way of life and fighting abroad for a cause is not new to Americans. What is new is America's willingness to give up some of its civil liberties and surrender some of its rights. During the implementation of the Presidential directivities, civil liberties will be challenged. We have already forfeited some liberties as a result of the President's call for mobilization of national guardsmen and reservists to improve the security of the nation's critical information infrastructures. Shortly after 11 September 2001, national guardsmen were called to active duty to assist in securing airports, federal buildings, nuclear power plants, power grids, and other critical infrastructures. Laws were challenged as these objectives were accomplished. The President has called for a review of policies that enhance security of the critical information infrastructure. By addressing current policies and shortfalls, the President has provided a means to fulfill the nation's goals outlined in the NSS: continuing to prosper through international markets, sustaining growth in the global economy, promoting democratic values, respecting human rights, and adhering to the rule of law.[6]

The challenges the nation faces in protecting the critical information infrastructure include everything from defending against physical destruction and psychological operations to cyber terrorism. America no longer has a single adversary to fight. The battle has become an asymmetric, non-kinetic fight which encompasses a global effort. Information operations strategy is controlled and guided by the U.S. Code of Law to protect our citizens' individual freedom. Presidential Decision Directives, regulatory and policy guidance, and Joint publications doctrine mandate strict conformance to the provisions of those laws. Other implications that cannot be ignored are limitations current laws have placed on anti-terrorist activities. A review of the IO infrastructures' vulnerabilities and operations in light of the present National Security Strategy (NSS), the Report of the Quadrennial Defense Review (QDR), The National Military Strategy (NMS), and Joint Doctrine for Information Operation (Joint PUB 3-13) publication identify the challenges that the U.S. must address in order to protect its critical information infrastructure.

QDR

The Quadrennial Defense Review (Sept 2001) outlines the military strategy for America's defense to prepare for uncertainties, overcome surprises, and ensure security. Regarding IO, the Quadrennial Defense Review (QDR) requires the military to "[Protect] the critical base of operation (U.S. Homeland, forces abroad, allies, and friends) and defeat Chemical, Biological, Radiological, Nuclear and Explosives (CBRNE) weapons and their means of delivery, [Assure reliability of] information systems in the face of attack and conduct effective information operations [Deny] enemy sanctuary by providing persistent surveillance, and [Leverage] information technology and innovation concepts to develop interoperable." [7]

PROTECT

Protecting the homeland has always been a priority for the U.S Army. Since suicide attacks are now the choice of destruction against the values that the U.S. represents, DOD is enhancing its ability to defend against terrorism. Terrorist groups and individuals such as Hezbollah and al-Qaida and individuals like Timothy McVeigh and Osama Bin-laden have chosen terrorist activities conducted by air, land and sea to advance their goals against the United States; therefore, Department of Defense has refocused its goals in defending America at home and abroad. The method these terrorists have used thus far in attacks against the U.S. and its friends have been bombings of various sorts. For example, terrorist employed a car bomb at the World Trade Center in 1993; fertilizer and a car bomb in the 1995 Oklahoma City bombing (although by an inside actor, Timothy McVeigh), and a truck bomb at Khobar Towers in 1998. We suffered an attack against the embassy in Africa. In 2000, the attack against the USS Cole was from the sea; and in 2001 an attack against the U.S. using U.S. aircraft and targeting key infrastructures. These attacks range from simple to complex, backed by millions of dollars spanning the entire geo-spatial (air, land and sea) dimension. Although the Army is charged with the protection of the nation's survival and deterrence of aggression, this charge has become a worrisome task because of little action, no budgetary authority, and no immediate plans to increase military manning, nor an internal plan to restructure. Yet, IO plays an important role in how the military plans to defend the nation against future terrorist attacks; after all, the Army's reason for existence is to fight and win the nation's wars.

ASSURE COMMUNICATIONS

Defining the enemy is another IO function that is becoming difficult as more users become familiar with computers. Rapid expansion of computers has resulted in an increased number of inexperienced users who create vulnerabilities due to their unfamiliarity with basic security

practices. Information Operations allow communicators to conduct offensive attack missions against adversarial forces desiring access to the network. These attack missions challenge the defense's ability to influence and protect information being passed throughout the network. The table below indicates a prediction of growth in computer usage, networks, and personnel who have the technical skills necessary to participate in a cyber attack. The last line of the graph shows software specialists who could be more harmful to the network than a maintainer and technical supporters. These individuals work with programs that require legitimate users to install software patches which ensure backdoor access to computer programs network has been blocked. This knowledge and ability qualify these individuals as insiders who could threaten the survival of the network. Constant monitoring, disciplinary action and security checks of these individuals are required to assure the safety of the network.

Category	15 Years Ago	1996	5 Years Hence
Personal Computers	Thousands	400 million	500 million
Local Area Networks	Thousands	1.3 million	2.5 million
Wide Area Networks	Hundreds	Thousands	Tens of thousands
Viruses	Some	Thousands	Tens of thousands
Internet Devices Accessing the World Wide Web	None	32 million	300 million
Population with the skills for a cyber attack	Thousands	17 million	19 million
Telecommunications Systems Control Software Specialists	Few	1.1 million	1.3 million

TABLE 1 GLOBAL TECHNOLOGY TRENDS

Information gained from The Report on the President's Commission on Critical Infrastructure Protection. Pg. 9

(Technical population data, programmers and telecommunications, 1982-2025, International Data Corporation, and e-mail and documents from the National Computer Security Center, National Security Agency, July 29,1997.)

ASSURE COMMUNICATIONS

Assuring communications during an attack requires integrity of everyone within the network. Enforcing compliance of systems policies, procedures and practices is one of the first responsibilities of an IO planner. Partnering with commercial vendors and other governmental agencies on efforts regarding state – of – the - art communications and technology development will also aid IO planners in improving the security of computers systems. Information warriors must constantly seek new ideas and philosophies in the conduct of information warfare.

DENY

In Joint Pub 3-58, military deception is defined as action taken to deliberately mislead adversarial military decision makers. Friendly military leadership must take specific actions that will contribute to the accomplishment of the friendly mission.

In order for deception to be achieved, execution of information assurance (IA) must control how well one can deny the enemy access to friendly information. Deception has been a key element to military success during conventional warfare, small conflicts, and during the Gulf War of 1991. As America continues to seek information dominance and superiority, America will likely be challenged by adversarial threats and attacks across the spectrum of warfare; therefore, the execution of IA is vital to accomplishing the mission.[8]

LEVERAGE TECHNOLOGY

During the 21st century, information technology will remain a vital component of Army transformation. The way information technology is infused in the plan will either accelerate or hinder the nation's progression toward security. The Army's Director of Command, Control Communications and Computers (DISC4) has established policies that accelerate communications efforts in protecting the network. The Director has coordinated with the Training and Doctrine Command (TRADOC) and designed training that allows communications technicians and other communications professionals to take courses and receive certification via a coordinated partnership with Microsoft, Hewlett Packard and Unix-based companies to stay proficient and to remain one step ahead of violators. The DISC4 web site offers more than a thousand titles in computer courseware. The DISC4 is also responsible for over five hundred course modules that can aid computer maintainers in their profession and assist commands in developing knowledgeable soldiers and civilians throughout the network. The courses are being taught at armories, reserve centers, home stations, combined training centers, deployed sites, and at the home station training institution. All of this training seeks to grow a smarter

workforce. The advantage of this concept is the Director's ability to reach the users, maintainers, and operators of the network. This is a proactive and responsive effort.

NATIONAL MILITARY STRATEGY (NMS)

The National Military Strategy (NMS) supports the President's National Security Strategy and the Quadrennial Defense Review (QDR) Report. "As we pursue the President's strategy for enhancing our security in this new era, the demand for military capabilities and skills is unlikely to diminish, both to deter and defeat aggression in two distant and overlapping Multiple Theater of Wars (MTWs), and in roles other than traditional warfighting."[9] One of the roles identified in the NMS that is essential to maintaining our military and civilian environment is the security of our critical information infrastructure which plays such a large role in our civilian prosperity and military security. The National Military Strategy states we must maintain our information superiority and protect it by both offensive and defensive means.[10]

JOINT PUBLICATIONS 3-13

This publication promulgates IO doctrine to accomplish the National Security Strategy (NSS). It defines IO objectives and offers details of offensive and defensive measures, giving overall guidance concerning IO planning. It also discusses organization and training issues. The defensive measures provide guidance on integration and protection of the critical information infrastructure. It also covers indications and warnings and provides restoration and operational attack procedures. It improves security of the critical information infrastructure. Figure 1 illustrates that defensive information operation procedures are constantly being performed during information operations process.[11] The following paragraphs explain offensive and defensive functions.

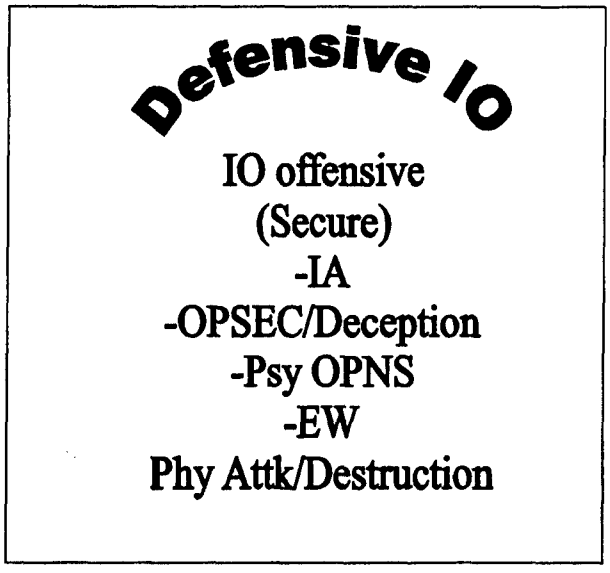

FIGURE 1

OPERATION SECURITY (OPSEC) AND DECEPTION

"Operation Security (OPSEC) and Deception were combined to convince Saddam Hussein of Coalition intent to conduct the main offensive using ground and amphibious attacks

into central Kuwait and to dismiss real indicators of the true Coalition intent to swing west of the Iraqi defenses in Kuwait and make the main attack into Iraq itself."[12]

Operation Security and Deception during Desert Storm caused the enemy to react and commit forces to areas not initially considered, thus leaving Saddam Hussein vulnerable to a central attack, thus giving the advantage to the American Coalition.

PSYCHOLOGICAL OPERATIONS (PSYOP)

Psychological Operations efforts are targeted at the government, their people and political organizations. The goal of PSYOP is to influence the will of the people and gain the people's confidence. During the initial attack against Afghanistan, the Afghanistan people's views of America were negative primarily due to the lack of knowledge the people possessed regarding the attack. The Taliban government and the leadership of al-Qaida tried to convince the people of Afghanistan that America was attacking the religious faith of the Afghan nation. The Taliban government and the al-Qaida network's goal was to gain support of the Afghan population, the political will of the people, to promote hatred towards any American effort in Afghanistan. Using PSYOP as a tool, America was able to reach the people through leaflets, food, broadcast coordination, use of coalition forces, and good deeds to prove America was not attacking their religious faith, but was attacking terrorists' activities. Unfortunately, Afghanistan's government supported terrorist networks and activities. The PSYOP efforts cast a brighter light regarding America's efforts in Afghanistan regardless of America's efforts or explanation. No country wants to be attacked, but the PSYOP efforts have paid off and proven to be an effective measure in America's efforts against terrorism.[13]

MILITARY DECEPTION

In the event of an attack against American forces, a commander must decide how he wants the adversary to react. A commander must also anticipate what the adversarial intention might be if he stages an attack or conducts certain military operations. America's actions must be convincing enough to cause the enemy to commit forces to deny America of her intent. Sun Tzu states "Now war is based on deception. Move when it is advantageous and create changes in the situation by dispersal and concentration of forces".[14] If deception is employed, it is heavily resource-reliant.

ELECTRONIC WARFARE

Gathering data on the electronic employment of the adversary's communications systems is part of electronic warfare. The adversary's systems may be jammed, or they may be targeted

by direct attack. Electronic Warfare consists of three subdivisions which contribute to offensive and defensive measures of employment.[15]

PHYSICAL ATTACK / DESTRUCTION

Physical attacks against the enemy yield a hard kill against the enemy's hardened structure and communications infrastructures.

CIVIL AFFAIRS

An information operation also requires America to employ her elements of power when cooperating with coalition government being targeted by terrorist groups. Used properly, Civil Affairs aids America in using the indigenous population to exploit America's goals. These measures involve actions taken against the adversarial forces to give advantages to America's offensive and defensive efforts.

INFORMATION OPERATIONS DEFENSIVE FUNCTIONS

A good defense has always served a good offense. In securing our infrastructure we need operators that think defensively. Operators must be retrained in basic skills for protecting the network. They must seek ways to stay ahead of the adversarial forces. The defensive postures of Information Operations consist of protection through tailored intelligence programs to ensure Integrity and restoration of the information systems. [16]

DEFENSIVE INFORMATION OPERATIONS

Regulations put a higher priority on defensive operations: "Defensive Information Operations ensure the necessary protection and defense of information and information systems upon which joint forces depend to conduct operations and achieve objectives."[17] Defensive operations consist of integrating procedures and protective measures to support operations within a multinational force arena that allows sharing information to enhance synchronization, timely response, and unity of effort. Information Assurance (IA) is a critical phase of this process. Information Assurance provides protection of our systems by applying five basic principles through the use of technology and multilevel security procedures and software. The processes to ensure system integrity are authentication, non-repudiation (undeniable proof of participation), availability, confidentiality, and integrity (protection from unauthorized change). Four interrelated processes make up Defensive Information Operations. Those processes are information environment protection (IEP) attack detection, restoration of

capability, and attack response. A brief explanation of how these processes may be used at the strategic level shows how defensive IO supports all phases of military operations.[18]

These measures involve actions taken against the adversarial forces to give advantages to our offensive and defensive efforts.

INFORMATION ENVIRONMENT PROTECTION (IEP)

The ultimate goal of this process is to protect every phase of the information environment to include the hardened structure, types of process to include video, hardcopy message, voice, electronic warfare (EW), imagery, and computers - along with such means as satellites, microwave, telephone, radios, and human means. This process is perhaps the most difficult because the extent of protection must be identified and must remain functional throughout an operational mission.[19]

ATTACK DETECTION

Identifying, designing and developing techniques to mitigate vulnerabilities are crucial to safeguarding and protecting the networks. Reports and analyses are forwarded to law enforcement agencies and intelligence collectors to ensure timely and sufficient warning to take action to counter the adversarial intent.[20]

CAPABILITY RESTORATION

This third process involves redundant options that maintain operability from an alternate location that possesses technical capability greater than that of the subordinate sites. The alternate restoral facility uses automated intrusion detection systems, firewalls, and software to protect the network from exploitation. This process calls for analysis and knowledge of the system in order to protect, prevent, and restore communications in a timely manner.[21]

ATTACK RESPONSE

This is the final process of defensive information operations. This process in some ways replicates the offensive phase of IO; it involves the same processes but places emphasis on performing defensive measures. Key to this process of operation is education, training, and computer awareness. Other operations performed in this process are counter deception, intelligence surveillance, and command information input. By educating the participants in the procedures and on vulnerabilities, the command heightens computer awareness regarding protection of critical information. [22]

The military, like many federal agencies, will require more interagency cooperation within the government as well as private and commercial sectors to enhance and ensure the nation's security. All agencies must eliminate ambiguity and strengthen outmoded policy. The nation's military, federal agencies and commercial sectors must change procedures and policies to strengthen the security of the networks. An example of a stronger policy is to limit expansion of the network to such a rate that secure measures permit protection from unauthorized use or intrusion. Federal and non-governmental organizations must act positively by cooperating, conducting target assessments, planning and sharing information in order to defeat and secure the nation's critical information infrastructure against adversarial threats. The private sector must understand that they are targeted more because adversaries view them as having weaker policies and relaxed procedures. The private sector must also understand they are not immune to cyber intrusion.

The attack on America on 11 September 2001 identified weaknesses and a lack of survivability for the nation's critical information infrastructure. To prevent these weaknesses from occurring again, planners and system maintainers must renew their communications charter with a sense of urgency to correct the shortfall. We must truly secure the nation's critical information infrastructure. We must study how the terrorists took advantage of America's good nature and relaxed security practices. What's known today is that terrorists used several variables to accomplish their goals. The terrorists used aircraft as weapons of mass destruction to invade America's way of life and dreams, and violated the most sacred core of America's being - life, liberty, and the pursuit of happiness. In terms of resources, they targeted the airline industry which caused America to lose thousands of precious lives as a result of their cowardly acts. The terrorist activities on 11 September 2001 taught America and the world that terrorism has no friends. Terrorism has forced American leaders, military strategists, visionaries and military planners to focus inward on the security of the nation's critical information infrastructure. Terrorists left America emotionless and numb, as they ripped through the fabric of America by attacking the nation's psychological realm.

The desire for dominant military knowledge in the information field depends on Department of Defense's ability to synchronize its efforts with other governmental and non-governmental organizations to establish a common understanding of the vulnerabilities to the nation's critical information infrastructure. The government must also protect documentation that identifies security weaknesses of the critical information infrastructure. These documents are often sought by adversarial parties to gain insight on how to attack the infrastructure. This

information must be shared and protected between the government and non-governmental agencies. All agencies must work to devise recommendations to ensure America's success.

INFORMATION OPERATIONS (IO) INFRASTRUCTURE VULNERABILITIES AND SHORTFALLS

Although offensive and defensive measures have been devised to protect the information infrastructures, several challenges have been identified in the NSS, QDR, NMS or Joint publications documents pertaining to shortfalls in protecting the critical information infrastructure network across the nation's critical communications and power grid structures. Information Operations vulnerabilities range from human neglect, unauthorized users, hackers, natural disasters, and terrorist activities. These vulnerabilities occur due to the ease with which the infrastructure can be disrupted. The President's Commission on Critical Information Infrastructure Protection has indicated that there is "little in the way of special equipment required to launch IW attacks on our computer systems; the basic attack tools - computers, modems, telephones, and software – are essentially the same as those used by hackers and criminals."[23] A recent article titled *Info Warriors' Given New Clout*, estimates that, "Today there are over 400 registered terrorist groups around the world and many have chosen asymmetric approaches –such as info war— to disrupt activities in the U.S. and other nations. With their abilities to strike back constrained by law, U.S. military forces and the FBI can only defend, then exploit any attackers' weaknesses."[24] Dhillon and Smith confirm this in *Defense Information Operations and Domestic Law:* "Limitations on government investigative techniques must be reviewed and rewritten to allow for timely retrieval of prosecutable data now more than ever, because there are more users relying on or desiring access to the Internet." More governmental oversight of the Internet impacts on the civil liberties of all users due to the violation and abuse of a few users. Our laws have not kept pace with Internet use or with the inventiveness of unscrupulous users. The commercial sector, which loses money from information leaks and attacks, has developed means to combat users who take advantage of company proprietary information. The commercial sector has found legal loopholes that can be applied in protecting their network, but the government is not able to use those same legal loopholes. As Dhillon and Smith observe, "[t]he protector of our national security should not be free to take advantage of these gaps and loopholes, as they are charged not only with ensuring that their conduct is consistent with the letter and spirit of our laws, but that they also act consistent with our constitutional values."[25]

ADMINISTRATIVE AND LEGAL CHALLENGES IN ADDRESSING INFORMATION INFRASTRUCTURE

The most misunderstood element of power is information. The term information is so elusive that it presents administrative and legal challenges in addressing how we should protect the information infrastructures. Information is also mentioned in numerous policy documents, but we are challenged in determining whether information should be represented by a cabinet level position. Organizational management, technical oversight, and funding issues constantly surface in discussions of management of information.

Likewise, there are legal challenges confronting IO in maintaining the security of the nation's critical information infrastructure. Some of the legal challenges prevent federal agencies from identifying the immediate location of the hacker without a warrant. These challenges keep federal agencies from finding perpetrators who have infiltrated the system. There are also laws that prevent timely investigation and prosecution of illegal acts.

Another obstacle to the government's timely intervention of illegal use or abuse of an IO system involves the Fourth Amendment, which "[p]lace limits upon the government's ability to intrude into the lives of the people."[26] Current interpretation of the Fourth Amendment views the computer as a storage medium and protects the personal information stored on one's computer. Unless legal authorities have probable cause, without a search warrant they cannot gain access to the information stored on an individual's personal computer. This limits authorities' ability to conduct timely investigations. As investigators seek to obtain a search warrant, the perpetrator has time to destroy evidence.

A third frequently noted obstacle is the Computer Fraud and Abuse Act. According to that law, it is often impossible to determine at the outset if an intrusion is an act of vandalism, organized crime, domestic or foreign terrorism, economic or traditional espionage, or some form of strategic military attack. The only way to determine the source, nature, and scope of the incident is to gather information from victim sites and intermediate sites such as Internet Service Providers and telecommunications carriers."[27] Yet this same law prevents the government from tracking the path of a violator back through the Internet. The government is only allowed to "hack-back" to the last of the violator's relay stations without a search warrant.

Finally, there is the Posse Comitatus Act (PCA). This law reinforces "...our deeply rooted belief in the division between civil law enforcement and military actions."[28] It prevents improper use of military assistance to enforce civil law. When there is an intrusion to military Internet sites or systems, this law hinders the military's ability to conduct any kind of investigation into the attack on its system. The military can defend its systems, but the military cannot undertake

action against a perpetrator. Such action can be undertaken only by appropriate civil authorities.

ORGANIZING IO STRATEGICALLY

"Of the four great instrumentalities available to nations for influencing the world around them –Diplomacy, Armed Forces, Money and Information – the last is both the most powerful and the least understood."[29]

When asked if the United States is prepared to protect itself against a cyber attack, the Nation's lead agency spokesmen respond doubtfully. Michael Jacobs, the National Security Agency (NSA) Director of Information Assurance responded simply, "No." Matha Stansell-Gram, the Chief Justice Department Computer Crime and Intellectual Property Director admitted, "Cyber threat is a huge interdisciplinary and multifaceted problem." She goes on to admit that agencies among the federal government, law enforcement, intelligence, and defense communities do not work well together when it comes to fighting cyber crimes or protecting the cyberspace.[30]

For more than 100 years, America's government has studied ways to protect and defend America's national values and national interest to ensure the success and goals of the constitution. The nation's values are the moral fabric that makes America the symbol of freedom to the rest of the world. The moral fabric of the nation is bound up in the guarantee of life, liberty, pursuit of happiness, economic prosperity, and individual rights. Threats to the livelihood and fabric of America's belief system must not be taken lightly; they must constantly be analyzed. We must remain ready and willing to use elements of power to gain the advantage over any adversary who is seeking to threaten America's survivability.

Organizing strategically aligns our information elements of power with how the government is structured to influence behavior in the diplomatic, economic, and military environments. In our government, three of the four elements of power are represented by a cabinet level position. Those elements of power are diplomatic or political, which is represented by the cabinet position of the Secretary of State. The economic element of power is represented by the Department of Commerce. The military element of power is represented by Department of Defense. The only element of power not represented by a cabinet level position is information. As the government continues to restructure in preparation for Homeland Defense, it should consider using the office of Homeland Defense to provide organizational, political and technical oversight in managing shortfalls identified in the information realm of these elements of power.

NATIONAL COMMAND AUTHORITY AND THE NATIONAL SECURITY COUNCIL

The National Command Authority and the National Security Council as well as many other agencies frequently employ information as an element of power. There are numerous agencies within our government that employ information as an element of power, but these agencies exist with different authority, different focus, and different missions. The problem most often encountered as a result of our pervasive use of information operations is that there is no strategic vision for the employment of information as an element of power in support of the nation's goal. Nye and Owens claim, "Knowledge, more than ever is power. The one country that can best lead the information revolution will be more powerful than any other. For the foreseeable future, that country is the United States. America has apparent strength in military power and economic production. Yet, its more subtle comparative advantage is its ability to collect, process, act upon and disseminate information as an edge that will almost certainly grow in the next century." [31] The authors of The Information Age see a capability of information that is not being exploited by our government. These authors suggest that the U.S. intelligence advantages are far superior to those of any other nation; they believe exploiting these advantages will give the U.S. the advantage it needs to defeat adversarial activities.

What these authors do not say is that adversarial forces are aware of the American appetite for more information, so the adversarial forces are seeking ways to deny America access to their information. To respond effectively and defeat the adversarial forces, America must first concentrate on improving its information infrastructure organization. It is extremely confusing and disconnected at the highest levels our government as to who is in charge of the information infrastructure organization. At the national level, security guidance comes from the National Command Authority to the National Security Council down to the Cabinet Secretaries; however from that point the organizational structure becomes blurred. In an effort to establish ownership in the process, the President signed Executive Order 13231 on October 16, 2001, Critical Infrastructure Protection in the Information Age. This executive order advocated law "in order to ensure protection of information of information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems, in the information age."[32] As policy, the President tasked the Executive Branch, Office of Management and Budget (OMB) to oversee the implementation and execution of the executive order. As the lead agency, OMB has the responsibility to keep the President informed of all deficiency and shortfalls within the critical information infrastructure. The policy also tasks the Director of Central Intelligence (DCI) to "oversee, develop, and ensure implementation of policies, principles, standard, and guidelines for the security of information systems that support

the operations under their respective control. In consultation with the Assistant to the President for National Security Affairs and the affected departments and agencies, the Secretary of Defense and the DCI shall develop policies, principles, standards, and guidelines for the security of national security information systems that support the operations of other executive branch departments and agencies with national security information." [33] This organizational structure is graphically displayed in Figure 2.

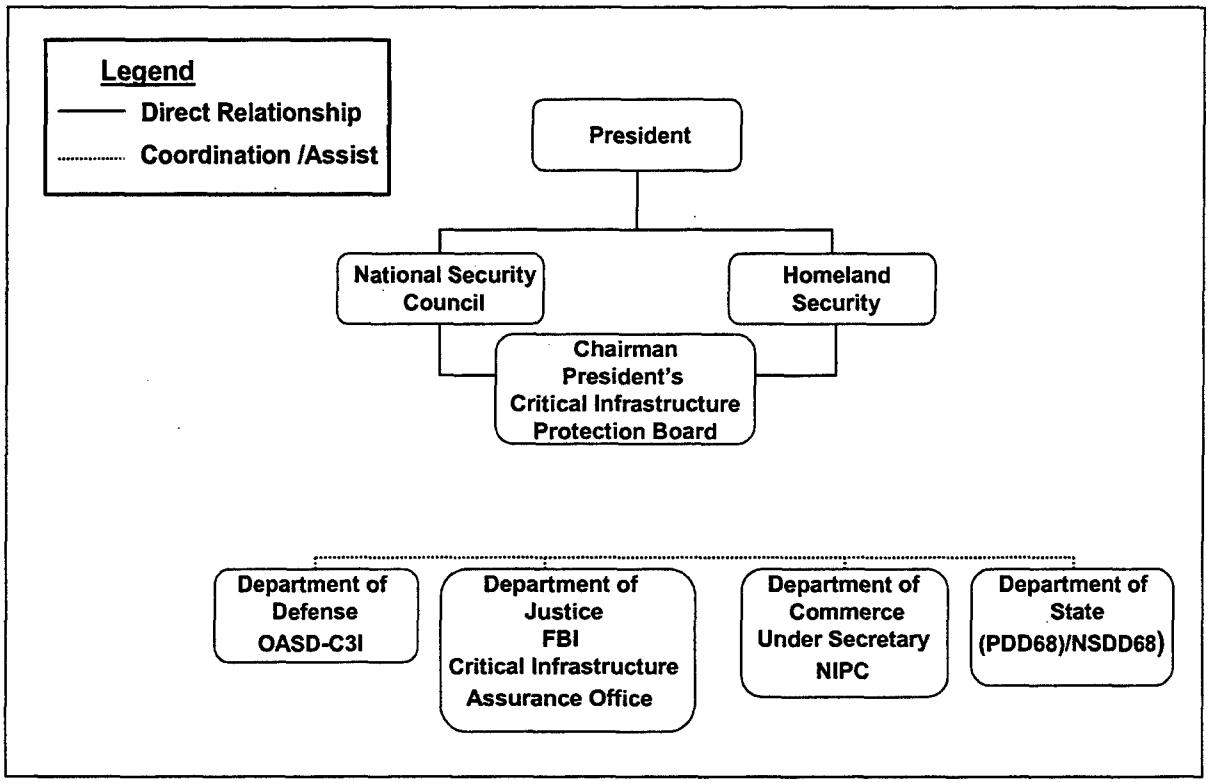

FIGURE 2 NATIONAL LEVEL ORGANIZATIONAL CHART

The flowchart shows a robust top level organizational structure the nation requires to ensure all efforts are directed toward a single strategic goal. The dotted line indicates a level of coordination and assistance required between the department heads and the civil sector to ensure protection and compliance. The newly enacted Critical Infrastructure Protection Board notwithstanding, the ultimate responsibility for managing the critical information infrastructure still rest with department heads and the private sector organizations. As a result of this newly enacted executive order, there are concerns that IO policies or implementation of security guidelines are not being adhered to either within the government or the private sector. This policy calls for the government and the private sector organization to become more responsible for the security of the information infrastructure. Improving the security of the information

infrastructure will require the involvement and training of every user at various levels of the government and the private sector. Using information as a true element of power will require additional Presidential mandate, guidance, and policy changes. These mandates must comply with and ensure the execution of the government's critical information infrastructure mission. In Digital Diplomacy, Wilson Dizard observes that "Unlike other countries the American communications and information sectors have historically been controlled by private firms, not by public agencies. U.S. companies routinely invoke First Amendment principles in resisting government control over their activities. It took almost a century after Samuel Morse's invention to pass a national law, the Communications Act of 1934, which mandated mild regulatory restraints on the telecommunication industry."[34] The nation cannot wait another century before addressing legal issues concerning the security and protection of the critical information infrastructures.

Protecting the critical information infrastructures will arouse the President and the nation's citizens' concern regarding the infringements of civil liberties. The challenge the nation's diplomatic leaders and citizens will face in protecting the infrastructures is to find a common ground of understanding that does not violate the right of the public, but equally protects the security of the Nation's critical infrastructures. Failure to find a common ground will be devastating to the greater welfare of America.

Winning the confidence of the American public will require the nation's leaders to be forthright in their decision and policies. In the past, the nation's political leadership has paid lip service to securing the critical information infrastructure. For example, in 1997, President Clinton indicated a desire to create a Homeland Security Directorate (HLSD). The focus of the HLSD would be to ensure the safety and security of America's infrastructures and territory. Due to the many challenges the Clinton administration faced, little emphasis was given to this request. But the 11 September 2001 terrorist attack quickly revived debates and interest in defending the country against asymmetric threats. In February 2001, Army War College Professor Joblonsky predicted "In the future, nations will wage offensive information warfare on another state's computer system targeting assets ranging from telecommunications and power to safety and banking."[35] It's not in the future that we are witnessing more attacks and threats to our information infrastructures. These threats and attacks are more frequent and direct today than ever at disrupting the economy and prosperity of America's way of life. In 1997 a Swiss research report revealed "...A total computer breakdown would kill banking activities after two days, commerce after two and half days, modern factories in five days and insurance businesses in five and a half days."[36]

The U.S. cannot afford to remain passive in securing the information infrastructure. The nation's leaders must take an aggressive role toward establishing structure and organization for critical base operations. The terrorist attacks against the World Trade Center, the Pentagon, and the nation's airlines cost America thousands of lives, brought the airlines to a halt, disrupted the headquarters of the greatest military power in the world, altered the thinking of the most powerful government in the world, and sent the nation's people into shock. Will it take another terrorist attack to reveal the nation needs to strategically organize its information infrastructure to prevent a cyber attack against the nation's critical information infrastructure? This is a question that must be answered by our government if we are to defeat any future attacks on our infrastructures. A key factor for the government is how it will reorganize and partner with the commercial infrastructure counterparts. The government must establish clear national goals and structure if a partnership is to be developed between the government and industry. To address these issues we look to the U.S. Commission on National Security.

U.S. COMMISSION ON NATIONAL SECURITY

The U.S. Commission on National Security during the 21st Century (the Hart-Rudman Commission) proposed a new National Homeland Security Agency. The recommendation builds on existing structure of Federal Emergency Management Act (FEMA), Coast Guard, Custom, and other agencies. Under Homeland Security, the Commission calls for a director responsible for protection of the Critical Information Infrastructures. "Two bills have been introduced so far in the 107th Congress addressing Homeland Security. The first bill, H.R. 1292, the Homeland Security Strategy Act of 2001, calls for the President to develop a Homeland Security Strategy that protects the territory, critical infrastructure, and citizens of the United States from the threat or use of chemical, biological, radiological, nuclear, cyber, or conventional weapons" and the second bill, "H.R. 1158 would establish a National Homeland Security Agency."[37]

The Congressional Research Service document addressing restructuring of the Bush Administration continue to debate the merit of establishing a government-wide Chief Information Officer (CIO), whose responsibilities would include protection of all federal non-national security-related computer systems, and coordination with the private sector protection of privately owned computer systems. The report stated the Bush Administration decided not to create a separate federal CIO position, but to recruit a Deputy Director of the Office of Management and Budget (OMB), that would assume an oversight role of agency CIOs. The rationale for this decision was a desire to keep agencies responsible for their own computer security.[38]

With the continued exploitation of information and global connectivity of the world, the speed with which an enemy can impact the will of a nation is greater than ever imagined. Despite technological developments, we are unable to locate Osama Bin Laden or members of the al- Qaeda leadership in the caves of Afghanistan. It has proven difficult to predict their next attacks or the magnitude of the attacks. Geography, distance, time and space are all factors once used to measure spatial separation between the friendly and the antagonist. Today the antagonist can be anywhere and devise practically any means to disrupt the Nation's national information infrastructure. Asymmetric warfare is as ambiguous as management of information. So where do we go from here?

PROPOSED RECOMMENDATIONS

President Bush should use the Office of Homeland Security (HLS) to provide technical oversight, budgetary guidance, and policy on securing the nation's critical information infrastructures.

Further, the President should establish within the HLS office a single lead agency that is responsible for coordinating with the private and public sectors to ensure security of those infrastructures germane to the health of the nation's information resources. Congress should enact legislation to give the HLS agency authority to oversee the execution of the national policy and develop strategy that applies across the public domain to assure defense of the nation's systems of telecommunications, energy, financial services, manufacturing, water, transportation, health care, and emergency services. The laws must be specific enough to hold the public or private organizations accountable for violations in these areas.

Department of Defense should be designated as the interim agency to oversee the implementation of policy and guidelines in support the HLS executive branch, then transfer those responsibilities within a specified time, to the Homeland Security Director.

Finally, the President should establish a federal CIO position to emphasize protection of the information infrastructure. The CIO would provide budgetary guidance, technical oversight, and enforcement of national policy and ensure compliance of the critical information infrastructure.

WORD COUNT: 6681

ENDNOTES

[1]William J. Clinton, A National Security Strategy for a Global Age (Washington, D.C.: The White House, December 2000), 9.

[2] Ibid.

[3] The Presidential Decision Directive - PDD 39, "U.S. Policy on Counterterrorism" (Washington, D,C.: The White House, June 1995); available from <http://www.fas.org/irp/offdocs/pdd39.htm>; Internet; accessed 6 March 2002.

[4] The Presidential Decision Directive – PDD 62, "U.S. Policy on Unconventional Threats to Homeland and Americans Overseas" (Washington, D.C.: The White House, May 1998); available from <http://www.fas.org/irp/offdocs/pdd-62.htm>; Internet; accessed 6 March 2002.

[5] The Presidential Decision Directives – PDD 63, "U.S. Policy on Critical Infrastructure Protection" (Washington, D.C.: The White House, May 1998); available from <http://www.fas.org/irp/offdocs/pdd-63>; Internet; accessed 6 March 2002.

[6] Clinton, 9.

[7] Donald H. Rumsfeld, Quadrennial Defense Review Report (Washington, D.C.: U.S. Department of Defense, September 2001), 43.

[8] Department of the Army, Doctrine for Joint Operational Deception Joint Publication 3-58 (Washington D.C.: U.S. Department of the Army, 31 May 1996) v.

[9] Clinton, 27.

[10] John M. Shalikashvili, National Military Strategy of the United States of America Shape, Respond, Prepare Now: A Military Strategy for a New Era (Washington, D.C.: U.S. Department of Defense, September 1997), 17.

[11] Department of the Army, Joint Publication for Operational Deception, Joint Publication 3-13 (Washington, D.C.: U.S. Department of the Army, 9 October 1998), 8.

[12] Ibid., II-3.

[13] Ibid., II-4.

[14] Sun Tzu, The Art of War (New York: Oxford University Press, 1963), 106.

[15] Department of the Army, Joint Publication for Operational Deception, Joint Publication 3-13 (Washington, D.C.: U.S. Department of the Army, 9 October 1998), II-4

[16] Ibid., III-1.

[17] Ibid., III-1.

[18] Ibid., III-3.

[19] Ibid., III-7.

[20] Ibid., 12.

[21] Ibid., 12.

[22] Ibid., III-14.

[23] Robert T. Marsh, Critical Foundations: Protecting America's Infrastructures, The Report of the President's Commission on Critical Infrastructure Protection (Washington, D.C.: 1997) ,9.

[24] William B. Scott, "Info Warriors' Given New Clout," (February 1999): 2 [database on-line]; available from UMI ProQuest, Bell and Howard; accessed 21 September 2001.

[25] Joginder S. Dhillon and Robert I. Smith, "Defensive Information Operations and Domestic Law: Limitations on Government Investigative Techniques," (2001): 1 [database on line]; available from UMI ProQuest, Bell and Howell; accessed 21 September 2001.

[26] Ibid.

[27] Ibid.

[28] Ibid.

[29] Ithiel de Sola Pool, Quoted in Wilson Dizard Jr, Digital Diplomacy: U.S. Foreign Policy in the Information Age (Wesport, CT: Praeger 2001), 1.

[30] "Cyber Terrorism: U.S. Cyber Defenses Remain Weak, Official Says," National Journal's Technology Daily, 20 December 2001, (159 words) [database on-line]; available from Lexis-Nexis, Reed Elsevier; accessed 19 Mar 2001.

[31] Joseph S. Nye, Jr. and Williams A. Owens, "America's Information Edge," Foreign Affairs, March/Apr 1996, 20.

[32] Executive Order 13231, "Critical Infrastructure Protection in the Information Age" (Washington, D,C.: The White House, October,2001); available from <http://www.ncs.gov/image-files/eo-13231.htm>; Internet; accessed 26 March 2002.

[33] Ibid., 2.

[34] Wilson Dizard Jr., Digital Diplomacy: U.S. Foreign Policy in the Information Age (Westport, CT.: Praeger, 2001), 113.

[35] David Jablonsky, "National Power," in U.S. Army War College Guide to Strategy, ed. Joseph R. Cerami and James F. Holcomb, Jr. (Carlisle Barracks, PA, U.S. Army War College, 2001), 99.

[36] Muller-gulland, Niels, "Information Operations - Challenge or Frustration," Military Technology, 4 December 1997, 89.

[37] John D. Moteff, Critical Infrastructures: Background and Early Implementation of PDD-63 (Washington D.C.: The Library of Congress, Congressional Research Service, 2001) 16.

[38] Ibid.

BIBLIOGRAPHY

Bush, George W. Critical Infrastructure protection in the Information Age. Executive Order 13231 Washington, D,C.: The White House, October,2001. Available from <http://www.ncs.gov/image -files/eo-13231.htm>.Internet. Accessed 26 March 2002.

Clinton, William J. A National Security Strategy for a Global Age. Washington, D.C.: The White House, December 2000.

_____. U.S. Policy on Counterterrorism. The Presidential Decision Directive - PDD 39 Washington, D,C.: The White House, June 1995. Available from <http://www.fas.org/irp/offdocs/pdd39.htm>. Internet. Accessed 6 March 2002.

_____. U.S. Policy on Critical Infrastructure Protection. The Presidential Decision Directive - PDD 63. Washington, D.C.: The White House, May 1998. Available from <http://www.fas.org/irp/offdocs/pdd-63>. Internet. Accessed 6 March 2002.

_____. U.S. Policy on Unconventional Threats to Homeland and Americans Overseas. The Presidential Decision Directive - PDD 62 Washington, D.C.: The White House, May 1998. Available from <http://www.fas.org/irp/offdocs/pdd-62.htm>. Internet. Accessed 6 March 2002.

"Cyber Terrorism: U.S. Cyber Defense Remain Weak Official Says." National Journal's Technology Daily, 20 December 2001, (159 words). Database on-line. Available from Lexis-Nexis, Reed Elsevier. Accessed 19 March 2001.

Dhillon, Joginder S. and Robert I. Smith. "Defensive Information Operations and Domestic Law: Limitations on government Investigative Techniques," (Winter 2001): 1. Database on-line. Available from UMI ProQuest, Bell and Howell. Accessed 21 September 2001.

Dizard, Wilson, Jr. Digital Diplomacy: U.S. Foreign Policy in the Information Age. Westport, CT: Praeger, 2001.

Jablonsky, David. "National Power." In U.S. Army War College Guide to Strategy, ed. Joseph R. Cerami and James F. Holcomb, Jr., 87-106. Carlisle Barracks, PA, U.S. Army War College, 2001.

Marsh, Robert T. Critical Foundations, Protecting America's Infrastructures, The Report of the President's Commission on Critical Infrastructure Protection. Washington, D.C.: 1997.

Moteff, John D. Critical Infrastructures: Background and Early Implementation of PDD-63. Washington, D.C.: The Library of Congress, Congressional Research Service, 2001.

Niels, Muller-Gulland. "Information Operation - Challenge or Frustration." Military Technology, 4 December 1997, 89.

Nye, Joseph S. and Williams A. Owens. "America's Information Edge." Foreign Affairs, 75 March / April 1996, 20.

Pool, Ithiel deSola. Quoted in Wilson Dizard Jr., Digital Diplomacy: U.S. Foreign Policy in the Information Age, 1. Westport, CT: Praeger, 2001.

Rumsfeld, Donald H. Quadrennial Defense Review Report. Washington, D.C.: U.S. Department of Defense, September 2001.

Scott, William B. "Info Warriors' Given New Clout." (Winter 1999): 2. Database on-line. Available from UMI ProQuest, Bell and Howell. Accessed 21 September 2001.

Shalikashvili, John M. National Military Strategy of the United States of America Shape, Respond, Prepare Now: A Military Strategy for a New Era. Washington, D.C.: U.S. Department of Defense, September 1997.

Sun Tzu. The Art of War. New York: Oxford University Press, 1963.

U.S. Department of the Army. Doctrine for Joint Operational Deception. Joint Publication 3-58. Washington D.C.: U.S. Department of the Army, 31 May 1996.

_____. Joint Publication for Operational Deception. Joint Publication 3-13. Washington, D.C.: U.S. Department of the Army, 9 October 1998.